IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CURLING PLAINTIFFS' REPLY IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

TABLE OF CONTENTS

I. INTRODUCTION....1

II. STATEMENT OF FACTS....3

A. The Key Facts Are Beyond Dispute....3

B. The Election Integrity Community Does Not Support the Proposed Election System....4

C. BMDs with Barcodes Are Not Reliably Secure Because They Expose Voters to Undetectable Vote Manipulation....8

i. Not "if," but "when"....8

ii. Georgia's Proposed Election System Cannot Prevent, Detect, or Recover from Likely Attacks on BMDs....10

iii. Defendants Essentially Concede that the Intended BMDs Are Vulnerable and Focus on Irrelevant Issues....15

D. Aspects of the DRE/GEMS System Will Continue to Threaten the Proposed Election System....17

III. ARGUMENT....18

A. Plaintiffs Have Demonstrated the Severe Burden the Proposed Election System Will Impose on Their Right to Vote....18

B. Defendants Have Identified No Compelling State Interest that Outweighs the Substantial Burden on Plaintiffs' Rights....19

C. Defendants Fail to Show Any Burden....20

D. Curling Plaintiffs' Proposed Relief Would Best Secure the Rights of Voters with Disabilities....22

E. Defendants Recycle Arguments This Court Already Has Rejected or that Will Be Litigated as Part of the Motion to Dismiss....27

F. Fulton County Recycles Already-Rejected Arguments 28

i. Fulton County, as well as State Defendants, Can Provide Plaintiffs' Requested Relief 29

ii. Curling Plaintiffs Do Not Seek a "Second Bite at the Apple" 29

IV. CONCLUSION 30

TABLE OF AUTHORITIES

Cases

Anderson v. Franklin Inst.,
185 F. Supp. 3d 628 (E.D. Pa. 2016).....27

Burdick v. Takushi,
504 U.S. 428 (1992) 18

Curling v. Kemp,
334 F. Supp. 3d 1303 (N.D. Ga. 2018) 18, 19

Curling v. Sec'y of Ga.,
761 F. App'x 927 (11th Cir. 2019).....19

Edge v. Sumter Cty. Sch. Dist.,
541 F. Supp. 55 (M.D. Ga. 1981), *aff'd,* 456 U.S. 1002 (1982) 29

McDonald's Corp. v. Robertson,
147 F.3d 1301 (11th Cir. 1998)..... 21, 28

National Fed'n of the Blind v. Lamone,
813 F.3d 494 (4th Cir. 2016).....26

Purcell v. Gonzalez,
549 U.S. 1 (2006) 20

Reynolds v. Sims,
377 U.S. 533 (1964) 20

Tennessee v. Lane,
541 U.S. 509 (2004) 26

Wexler v. Anderson,
452 F.3d 1226 (11th Cir. 2006).....19

Statutes

O.C.G.A. § 21-2-300(a)(2) 28

I. INTRODUCTION

Defendants make virtually no effort to defend the election system they actually intend to force upon Georgia voters across the state: BMDs that tabulate votes based on computer-generated, unreadable *barcodes*. Defendants barely acknowledge—much less defend—their use of barcodes, which both of their own handpicked election security experts advised against. It is undisputed that, in the Proposed Election System, voters cannot verify that what that system will tabulate is actually what they intended. This is unconstitutional, just as the Georgia legislature recognized in requiring a *voter-verifiable* election system.

Defendants again resort to misleading claims to defend the indefensible. They suggest that there was no non-barcode BMD option for Georgia to select. But two vendors offered Georgia EAC-certified BMDs that use human-readable text, not barcodes, to tabulate votes. Defendants also seek to normalize their conduct by claiming that 44 states use BMDs. This is misleading. None of those states currently uses BMDs as the primary election system statewide as Georgia intends to do. Most of them use hand-marked-paper ballots (HMPBs), with BMDs available for those voters who cannot mark ballots by hand, which is precisely what Curling Plaintiffs seek in Georgia.

Defendants' only real effort to defend the Proposed Election System is to argue that they will verify election results with audits. But this fails. Not only are barcode-based results not subject to meaningful audits, Defendants have provided no details for any—much less effective—risk-limiting audits; nor have they committed to such audits for each election statewide. They offer no more than vague and empty assurances, which cannot satisfy their constitutional duties.

Defendants' argument that Curling Plaintiffs' proposed relief would unlawfully discriminate against disabled voters is equally meritless. No law requires that all voters vote in the same manner, nor is that consistent with relief sought by the National Federation of the Blind—from which Defendants offer sworn testimony—in prior election-related litigation. The law requires reasonable accommodations for certain voters, which non-barcode BMDs are. The notion that all voters must use BMDs because a small number of voters need them is wrong.

Defendants focus their efforts on defending BMDs generally. But that issue is not before this Court. The only question this Court faces is whether *Georgia's Proposed Election System* is constitutional, a system that would force all voters across the state to cast their votes via barcodes that they cannot verify or even read. This Court already ordered Defendants to use hand-marked-paper ballots if they cannot implement a lawful election system for 2020, and it required them to

prepare for this default system with a pilot election this year. On November 12th 2019, Cobb County Board of Elections and Registration Director, Janine Eveler, spoke about the Cobb County HMPB pilot at a Board of Elections meeting and described multiple aspects of the pilot that she and her team were "a little bit surprised about and pleased about," while stating "the counties that were doing the ballot marking device pilot were dead in the water."[1] This Court should not permit Defendants to further deprive Curling Plaintiffs and all other Georgia voters of their constitutional right to vote. Defendants seek to replace one unlawful system with another. The Court should stop this and enforce the default system it ordered months ago and that already has been successfully piloted in Georgia.

II. STATEMENT OF FACTS

A. The Key Facts Are Beyond Dispute

Defendants repeatedly, and falsely, claim that the Proposed Election System provides a voter-verifiable ballot. (Opp. 5, 12, 39-40, 46.) But it is undisputed that the portion of the ballot that is tabulated is not voter-verifiable. Defendants'

[1] GA VOTERS FOR HMPBs, *Cobb HMPB Pilot*, YouTube (Nov. 15, 2019), https://www.youtube.com/watch?v=rL_4rihgbhc&feature=youtu.be. Poll watchers who observed BMD pilots in multiple polling places described widespread problems with the State's electronic pollbooks, ballot secrecy, and voter verification of ballots. *See* Supplemental Declaration of Rhonda J. Martin; Declaration of Elizabeth Throop; Supplemental Declaration of Jeanne Dufort.

BMDs print a 2D barcode and a written summary of voters' choices; however, their scanners will tabulate votes based on the barcodes, not the summaries. (Dkt. No. 658-2 ¶ 4.) Voters cannot read barcodes and no voter can verify whether a barcode accurately conveys his or her intended selections. (*Cf.* Dkt. No. 579 at 9 n.10.) This fact is undisputed and dispositive.

B. The Election Integrity Community Does Not Support the Proposed Election System

Defendants ignore the fact that both of their own election security experts, Drs. Michael Shamos and Wenke Lee, advised against the Proposed Election System. They have no explanation for why they disregarded that expert advice. They suggested to the Court that there was no non-barcode BMD for the State to choose in its procurement process and that there is no non-barcode BMD that is EAC-certified. (Dkt. No. 679 at 30:24-31:12, 43:25-44:5.) This is incorrect. At least two vendors, Hart Intercivic, Inc. and Clear Ballot Group, Inc., market EAC-certified BMD systems that do not tabulate votes via barcodes.[2] (Halderman Decl.

[2] U.S. Election Assistance Comm'n, *Certificate of Conformance: Hart Verity Voting 2.3* (Mar. 15, 2019), https://www.eac.gov/file.aspx?A=qfC3fSFkXPse3XTRqs1Po4ouXHWU1gQjo6Mbn9mSI78%3D; U.S. Election Assistance Comm'n, *Certificate of Conformance: ClearVote 1.5* (Mar. 19, 2019), https://www.eac.gov/file.aspx?A=zgte4IhsHz%2BswC%2BW4LO6PxIVssxXBebhvZiSd5BGbbs%3D.

¶ 17.) Hart submitted a bid for its Verity Duo system,[3] although for reasons it has never explained, the State did not evaluate that bid. And the State considered a bid that included Clear Ballot's ClearAccess BMDs.[4] The State rejected this bid without explanation.

Lacking support from their own election security experts, Defendants now turn to yet another expert, Dr. Juan Gilbert. But his expertise is not in election or even computer security, but rather in "computers generally," with a "focus on creating user interfaces." (Dkt. No. 658-3 ¶¶ 4, 14.) And he is hopelessly biased: Dr. Gilbert markets his own BMD Voting System, Prime III, that appears to use barcodes to tabulate votes, and he is currently promoting it to election officials across the country.[5] (*Id.* ¶ 16; *see also* Third Supplemental Declaration of Philip B. Stark ("Stark Suppl. Decl.") ¶ 28.) Dr. Gilbert has a substantial financial and

---

[3] Mark Niesse, *Georgia's Voting System Contract Attracts Bids from Large Election Companies*, Atlanta Journal-Constitution (Apr. 24, 2019), https://www.ajc.com/news/state--regional-govt--politics/companies-submit-confidential-bids-for-georgia-voting-system/SYsJ3vS3OxKYLKRw3BCDdK/.

[4] Ga. Sec'y of State, *Secure Voting*, https://sos.ga.gov/index.php/general/securevoting (last visited Dec. 16, 2019). What the State called the "SmartMatic" proposal included a proposal from ClearBallot for the Clear Ballot Group ClearVote 1.5 voting system, including ClearAccess BMDs, which do not produce a barcode or QR code ballot. (Cross Decl. Ex. A at 2, 6.)

[5] Prime III Voting System, http://www.primevotingsystem.com/ (last visited Dec. 16, 2019).

professional interest in encouraging the widespread adoption of BMDs.

Further, Dr. Gilbert's declaration is notable for what it omits: any rebuttal of the fact that the BMD-based Proposed Election System poses substantially greater risks to election security than Plaintiffs' proposed remedy of a HMPB system. (Appel Decl. ¶¶ 10-12.) In fact, Dr. Gilbert "do[es] not generally dispute" that the "use of barcodes generally increases the 'attack surface'" of a voting system. (Dkt. No. 658-3 ¶ 45.)[6] Neither does he opine that barcodes are necessary.

Dr. Gilbert instead resorts to the sweeping claim that "the advantages of a BMD system with respect to undervotes, overvotes, auditability, and accessibility weigh in favor of a BMD system," as compared to HMPBs. (*Id.* ¶ 32.) As Drs. Halderman and Appel—who actually are experts in election and computer security—explain, Dr. Gilbert overstates each supposed advantage of BMDs and each purported shortcoming of HMPBs. (Halderman Decl. ¶¶ 40, 42-46; Appel. Decl. ¶¶ 25-31.) In addition, none of the "advantages" Dr. Gilbert describes

[6] *See* Appel Decl. ¶ 32 ("BMD-marked paper ballots are insecure because: BMDs, like any computers, can be hacked (by alteration of their software program to cheat); if hacked, they can systematically change votes from what the voter indicated on the touchscreen when printed on the paper ballot; few voters will notice, and those that notice have *only* the mitigation that they might be able to correct their own ballots, not their neighbors; and finally, recounts or audits will see only the fraudulently marked paper. This is the central point of Professor Stark's and Professor Halderman's Declarations; and Professor Gilbert avoids disputing these central facts."); *see also generally* Stark Suppl. Decl.

depends on using barcodes. (Dkt. No. 658-3 ¶¶ 37-40.) When Dr. Gilbert mentions barcodes or QR codes at all, he describes circularly how they could be used to detect inconsistencies in the QR codes themselves, (*id.* ¶ 39(D)-(E), (G)), or acknowledges that Georgia's current implementation lacks features that would "provide a stronger audit trail to detect errors or malfeasance," (*id.* ¶ 39(F)). (*See also* Appel Decl. ¶ 31.) Dr. Gilbert never addresses the fact that HMPB systems are not exposed to the same inconsistencies or malfeasance possible in barcode-based BMD systems. (Appel Decl. ¶¶ 23-24.)

And Dr. Gilbert fails to address the critical vulnerability that election security experts, including Defendants' own, attribute to BMD-based voting systems: a BMD "may have a vulnerability that could be exploited to change votes" and that would go undetected. (Dkt. No. 615-2 at 2.)[7] As Dr. Lee advises, there is "now a well-developed consensus from cybersecurity researchers and

[7] Dr. Gilbert's opinion that "from a security perspective, it is better to have a diversity of voters using the same equipment rather than isolating a certain demographic of voters by type of equipment or voting process" exceeds his expertise. (Dkt. No. 658-3 ¶ 40(F).) Nevertheless, as Dr. Halderman explains, having all voters vote on BMDs would not prevent an attacker from implementing an attack that would alter votes only for visually impaired voters. (Halderman Decl. ¶ 34(a).) Having all voters use BMDs is also practically impossible because voters have a variety of needs. (*Id.* ¶ 48.) For example, absentee-by-mail voters would not be represented no matter the equipment used for in-person voting. (*Id.* ¶ 38.) Dr. Gilbert is wrong that forcing all voters to use BMDs would enhance the security of disabled voters' ballots, much less the entire election. (*Id.* ¶¶ 35, 47.)

computer scientists . . . that a secure voting system should work" by having voters hand-mark a paper ballot that is scanned and deposited into a secure ballot box. (*Id*. at 3.) Defendants' own *security* experts agree that the Proposed Election System is "much less desirable" than Curling Plaintiffs' proposed remedy. (Dkt. No. 615-2 at 2; *see also* Dkt. No. 554 at 56:13-57:2, 57:13-21.)

C. BMDs with Barcodes Are Not Reliably Secure Because They Expose Voters to Undetectable Vote Manipulation

Defendants draw false parallels between the vulnerabilities of HMPBs and BMDs. (Opp. 8-9.) Certain attacks, such as those on scanners, are theoretically similar. (*See id*.) But BMDs expand the types and magnitude of attacks because they (needlessly) inject computer software between the voter and the expression of her vote on the ballot. (Halderman Decl. ¶ 39; Stark Suppl. Decl. ¶ 30.)[8] Dominion's own Director of Product Strategy and Security admits "all computers can be hacked with enough time and access." (Dkt. No. 658-2 at ¶ 13.) Where barcodes are used to tabulate votes, the risk is especially acute—and avoidable.

i. Not "if," But "When"

Georgia's voting system and IT infrastructure will remain in the crosshairs

[8] Dr. Gilbert's claim that "[i]n essence, a BMD is nothing more than an ink pen," is remarkably misleading. (Dkt. No. 658-3 ¶ 60.) An ink pen is not a software-dependent machine that is susceptible to malicious attack (locally or *remotely*), and a ballot filled in by the voter is not equivalent to an un-readable barcode generated by a machine. (Appel Decl. ¶¶ 22-24; *see also* Halderman Decl. ¶ 7 n.7.)

in 2020 and beyond. As the Court and Defendants' own cybersecurity advisor, Ms. Payton, emphasized, this threat is not theoretical. (Dkt. No. 579 at 42; Dkt. No. 570 at 206:9-12.)[9] If attackers successfully breached any part of Georgia's prior DRE voting system that will continue to be used—*e.g.*, "the Secretary of State's computer network, the voter registration database software developed by PCC, Inc., and the non-'air gapped' computers used by state and county workers and outside contractors to transfer data into and out of the EMS"—"those attackers may continue to have access." (Halderman Decl. ¶¶ 9-10.) Defendants do not even argue that the Proposed Election System will withstand hacking attempts.[10]

Vulnerabilities with BMDs also include software bugs that need not be malicious. In November, a judge's race in Northampton County, Pennsylvania, suffered an apparent software bug with barcode-based BMDs that tabulated 164

[9] *See also* Declaration of Harri H. Hursti ¶ 16 (It is "probable that a system like Georgia's Dominion Voting System can and will be targeted by adversarial parties.").

[10] Defendants offer a feeble response to the demonstrated hacking of a Dominion ImageCast Precinct hybrid BMD and scanner machine at DEF CON. (Opp. 8-9.) Dr. Gilbert testified that the hacked scanner "***appear[ed]*** to be different than the system procured for Georgia," (Dkt. No. 658-3 ¶ 71 (emphasis added)), and Dr. Coomer testified that "all computers can be hacked with enough time and access," (Dkt. No. 658-2 ¶ 13). But tellingly, neither Dominion's Director of Product Strategy and Security nor Defendants claim that the security features of Georgia's machines will differ in any meaningful way from the one hacked this August.

votes out of 55,000 ballots for one candidate.[11] A manual recount showed the candidate actually received 26,142 votes and narrowly won.[12] A lawsuit seeks to enjoin the use of the BMDs before Pennsylvania's April 2020 primary elections.[13] Ironically, the size of the error in this race actually helped. If it had affected a relatively-small-but-dispositive number of votes, it almost certainly would not have been detected.[14] For example, the 2018 Georgia gubernatorial election was very narrowly decided and it was not audited or recounted.

ii. Georgia's Proposed Election System Cannot Prevent, Detect, or Recover from Likely Attacks on BMDs

Experts have articulated at least two kinds of attacks that are possible by altering the programming of BMDs. (Halderman Decl. ¶ 11.) Georgia's Proposed

[11] Nick Corasaniti, *A Pennsylvania County's Election Day Nightmare Underscores Voting Machine Concerns*, N.Y. Times (Nov. 30, 2019), https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html?searchResultPosition=1.

[12] *Id*. Defendants do not address how they would handle a recount if the Proposed Election System suffered a similar malfunction, including whether they would rely on the barcodes or the human-readable portion of the ballot.

[13] Joseph Marks, *The Cybersecurity 202: Lawsuit Seeks to Force Pennsylvania to Scrap These Electronic Voting Machines Over Hacking Fears*, Washington Post (Dec. 13, 2019), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/12/13/the-cybersecurity-202-lawsuit-seeks-to-force-pennsylvania-to-scrap-these-electronic-voting-machines-over-hacking-fears/5df27a70602ff125ce5b2fec/.

[14] An attacker is likely to use malware that would change only a fraction of the votes cast using BMDs. (Halderman Decl. ¶¶ 11-12, 21.)

Election System cannot prevent, detect, or recover from either.

In an "inconsistent barcode attack," the text summaries accurately reflect voters' selections, but some barcodes do not. Since the scanner reads the barcodes, it records erroneous votes, and an incorrect outcome of the election may be certified. (Dkt. No. 619-2 ¶ 6.) This kind of attack could evade both pre-election testing and parallel testing. (Halderman Decl. ¶ 14.) And while robust risk-limiting audits in which humans count only the text summaries might catch this kind of attack, Defendants' Proposed Election System cannot. (Opp. 13, 38; Dkt. No. 619-2 ¶ 7; Appel Decl. ¶ 21.)

Georgia law does not require—and Defendants have not committed to—statewide risk-limiting audits of every race by any date certain. Instead, as the Court noted, Georgia law requires only "some manner of auditing to evolve over the years to come." (Dkt. No. 579 at 139; *see also* Halderman Decl. ¶ 15 ("[A]n attacker could target any race in any election.").) Defendants have not identified any specific auditing procedures. It is thus still unclear, for example, whether Defendants will hand-count the text summaries or simply feed the barcodes through scanners a second time. (*See* Halderman Decl. ¶ 15 ("Georgia has not announced plans to perform any kind of audit that would compare the barcodes and the printed text.").) Ultimately, even if an audit detected barcode inconsistencies,

it might be impossible to determine the result of the race. (*Id*. ¶ 16; Stark Suppl. Decl. ¶¶ 5-7.)

Defendants assure the Court that they are "on track." (Opp. 22.) But Defendants' assurances that they will timely establish effective security and audit protocols hold no weight; they were "castigate[d]" by their own election security expert for conducting parallel testing on a single DRE out of the 27,000 used in the state, and insisted "nothing amiss happened in the gaping breach and exposure of the CES/KSU [server]." (Dkt. No. 579 at 54, 70.) Voters should not have to put blind faith in Defendants and vote in the shadow of such a breach.

In a "switched intent attack," both the text summaries and the barcodes differ in some part from some voters' intended selections. (Halderman Decl. ¶ 19.) Both the scanner and a post-election human auditor will record erroneous votes. (*Id.*) Although some portion of alert voters may detect a switch on their own paper printouts before casting them into the scanner, even Defendants do not argue that all or most voters are so alert and capable. Most importantly, Defendants' own cybersecurity expert explained that no post-election audit can detect a switched intent attack. "[I]t is meaningless to perform a post-election audit on printouts that cannot be guaranteed to be valid in the first place; the audit would just be 'garbage-in, garbage-out,' and perhaps worse, give a false sense of accuracy or legitimacy of

the election results." (Dkt. No. 615-3 at 2.) Even Dr. Gilbert admits: "The primary goal of having a paper ballot is to enable an audit to ensure the integrity of the election . . . . If the auditability of the ballots is compromised, then the audit/recount fails." (Dkt. No. 658-3 ¶ 39(B).)

The switched intent attack renders the Proposed Election System unconstitutional. The *only thing* that would signal this attack is if such an extraordinary number of voters caught the text summary errors and complained that election officials could not explain the phenomenon except as a systemic problem with the BMDs' programming. (Halderman Decl. ¶¶ 20-21.) That is extremely unlikely for three reasons.

First, the best available research in conditions designed to mimic an actual election indicates that only a small percentage of voters detect errors in the text summaries. (Halderman Decl. ¶¶ 23-30.) Even though Defendants quibble with the particulars of Dr. Halderman's research study,[15] they present no evidence that voters will detect errors at a high enough rate to reliably guard against a switched intent attack. Dr. Shamos testified that "a lot of people" will not verify their BMD printout, because many voters who carefully make their selections on the

[15] The study was provisionally accepted after peer review to appear next month in the IEEE Symposium on Security and Privacy. (Halderman Decl. ¶ 25.)

touchscreen will believe "I marked it right, it's going in there. . . . I don't have to check it." (Dkt. No. 554 at 210:18-20.) Dr. Lee likewise noted that "a large percentage of voters" do not verify the printouts. (Dkt. No. 615-2 at 2.)[16] Moreover, malware can selectively target voters less likely to detect or report errors or voters who take an unusually long time to vote. (*See* Philip Stark, *There is no Reliable Way to Detect Hacked Ballot-Marking Devices*, Univ. of Cal., Berkeley (2019), https://www.stat.berkeley.edu/~stark/Preprints/bmd-p19.pdf [hereinafter Stark Article] at 4 n.11, 6; *see also* Halderman Decl. ¶ 14.)[17]

Second, even if voters report errors, poll workers can only allow *those voters* to re-vote. Poll workers would have no way to verify voter allegations that the machine in fact "switched" any votes, and voters would have no way to prove them, without compromising their right to ballot secrecy by recording and disclosing their act of voting. (Halderman Decl. ¶ 21; Stark Article at 2.) As with

---

[16] *See also* Nat'l Election Defense Coal., *The National Election Defense Coalition Opposes Adopting Ballot Marking Devices as the Primary Method of Voting*, https://www.electiondefense.org/ballot-marking-devices?sfns=mo (last visited Dec. 16, 2019) [hereinafter "*NEDC Opposes BMDs*"] ("The evidence available indicates most voters are unlikely to catch errors in their computer-marked ballot summary, so misconfigured, malfunctioning or hacked BMDs could record votes incorrectly and the voter might not notice, or might notice and think it's the voter's own error.").

[17] Because he did not selectively target voters for manipulation, Dr. Halderman's experiment was actually more generous to BMDs in important ways than the threat model dictates an attacker would be in actual election conditions.

DREs, election officials will likely dismiss voter complaints as voter errors or one-off malfunctions. (*See, e.g.*, Dkt. No. 579 at 94-96.)

Finally, even if poll workers suspected a systemic attack, the only option would be to re-run the election. (Halderman Decl. ¶ 22; Stark Suppl. Decl. ¶ 39.) Not only would this be disastrous given the magnitude of and anticipated voter turnout for the 2020 elections, but how would this even be done?[18] To re-run elections on the same equipment would be pointless and only compound the problem. To re-run them with a HMPB system would only confirm that such a system should have been used in the first place. The loss of voter confidence would be enormous. Curling Plaintiffs' proposed relief is not vulnerable to these attacks, (Halderman Decl. ¶¶ 38-39)—and it happens to be much more cost effective and efficient for voters.

iii. Defendants Essentially Concede that the Intended BMDs Are Vulnerable and Focus on Irrelevant Issues

Defendants do not set forth any facts specifically defending the Proposed Election System's security or reliability from the vulnerabilities described by Defendants' own experts. Instead, they play up general acceptance of BMDs (not specifically barcode-based BMDs) by certain election authorities for certain

[18] Given the 2020 Presidential election, the impact would be at a *national* level.

limited purposes, *not for statewide elections for all voters*. Defendants, as they so often have, paint a remarkably misleading picture regarding the use of BMDs in other jurisdictions. (Opp. 2.) The truth is that only a relatively small portion of the country's many counties use BMDs and mostly only for disabled voters. The most recent available data shows that in November 2020, voters in only 12 percent of precincts in the United States (comprising 13.5 percent of registered voters nationwide) will mark ballots primarily by BMD. (Stewart Decl. Ex. 1 at 2G, 2O.) Meanwhile, voters in 72.5 percent of precincts will mark ballots primarily by hand. (*Id*. at 2E.) Moreover, the majority of precincts—63 percent—will use BMDs primarily for voters with disabilities. (Stewart Decl. Ex. 2 at 2I.) Only 12 percent of precincts will use BMDs for all voters. (*Id*. at 2G.) Defendants are incorrect: Georgia is absolutely an "outlier" in its plan to use BMDs for all voters in 2020 elections. (Opp. 2; *see also* Halderman Decl. ¶ 5.)

That vendors are currently promoting BMDs—and some counties are using them—indicates nothing about their reliability or lawfulness.[19] The same is true for the EAC certification, despite Defendants' suggestion to the contrary. (*See* Opp. 2, 13, 15, 25-27, 38.) Many states used DREs for many years and some still

[19] *NEDC Opposes BMDs*, *supra* note 16 (noting that BMDs are "very profitable for the vendors but very problematic for democratic elections.").

do. (Stewart Decl. Ex. 1 at 2Y (showing 16.9 percent of counties (or equivalent jurisdictional unit) will use DRES in November 2020.).) The EAC certified DREs for years.[20] But this Court rightly found Georgia's DREs unconstitutional. (Dkt. No. 579 at 130.) The same is true for its barcode-based BMDs.

D. Aspects of the DRE/GEMS System Will Continue to Threaten the Proposed Election System

Defendants understandably want to start from a blank slate, but the reality is that the Proposed Election System is not "completely separate from the old DRE/GEMs systems," as Defendants and their experts repeatedly claim. (Opp. 5 (citing Dkt. Nos. 658-2 ¶ 7; 658-3 ¶ 43).) At the very least, the Proposed Election System will be run by the same personnel using the same computer network and some of the same hardware as the prior system. (Halderman Decl. ¶ 9.) If the GEMS/DRE system has already been compromised, those same points of vulnerability could be used to infiltrate the Proposed Election System, and the tools Defendants tout are unlikely to detect or defend against such an infiltration. (*Id.*

[20] Georgia's prior Diebold DRE system was certified by the EAC by at least 2009 and does not appear to have been decertified to date. *See* U.S. Election Assistance Comm'n, *Certificate of Conformance: Premier Assure 1.2* (Aug. 6, 2009), https://www.eac.gov/file.aspx?A=Z%2bdvjI13643BIfjv4YpypeTuWZcl6Po9a9JDGZ17Kds%3d; U.S. Election Assistance Comm'n, *Voting Equipment: Withdrawn or Decertified Systems*, https://www.eac.gov/voting-equipment/withdrawn-or-decertified-systems/ (last visited Dec. 16, 2019).

¶ 10.) Defendants simply refuse to come to terms with this reality. That they have steadfastly refused for years to allow any security expert, including their own, to forensically examine DREs or GEMS servers betrays their concern—or worse, knowledge—that it has been compromised. (*See* Dkt. Nos. 570 at 216:10-217:18, 293:7-11; 565-7 ¶¶ 27, 45.) Defendants have admitted they will deliberately mislead the public, and this Court, about the insecurity of Georgia's election system to sustain the myth that the system is secure. (*See* Dkt. No. 647 at 3.)

III. ARGUMENT

A. Plaintiffs Have Demonstrated the Severe Burden the Proposed Election System Will Impose on Their Right to Vote

As this Court has twice found, Defendants' implementation of a system that exposes voters to the imminent risk that their vote will not be accurately counted burdens Curling Plaintiffs' Fourteenth Amendment rights. *Curling v. Kemp*, 334 F. Supp. 3d 1303, 1322 (N.D. Ga. 2018); (Dkt. No. 579 at 130). Defendants begin their argument with over ten pages on state sovereignty. (Opp. 23-30, 33-34, 36, 41.) This Court does not need a dissertation (an incorrect one, no less) on federalism after having already twice grappled with unique elections-related federalism issues under the flexible standard established in *Burdick v. Takushi*, 504 U.S. 428, 434 (1992). (Dkt. No. 579 at 129-150). This is especially true where the Eleventh Circuit already rejected Defendants' state sovereignty arguments as

frivolous. *See Curling v. Sec'y of Ga.*, 761 F. App'x 927, 932 (11th Cir. 2019).

Defendants' mischaracterized *Wexler v. Anderson*, 452 F.3d 1226 (11th Cir. 2006). (Opp. 33, 37.) The Court already distinguished *Wexler* on the basis that Plaintiffs presented sufficient evidence that their votes cast by DRE "may be altered, diluted, or effectively not counted on the same terms as someone using another voting method – or that there is a serious risk of this under the circumstances." *Curling*, 334 F. Supp. 3d at 1325. That reasoning still holds, because votes cast by BMDs are subject to the same risk of undetectable vote manipulation, as Defendants' own experts acknowledge. Dominion's barcoded-ballots make voter verification illusory and meaningful audits impossible. Defendants' assurances that they likely will develop and implement risk-limiting audits by November 2020 are of little weight, offer no protection for the March 2020 primary, and are not binding on the state or counties. Most importantly, the inevitability of switched intent attacks will make any audit—no matter how mathematically rigorous—"garbage-in, garbage-out." (Dkt. No. 615-3 at 2.) The Proposed Election System for 2020 is thus just as "non-auditable" as the DRE system this Court already found unconstitutional. (Dkt. No. 579 at 130.)

B. Defendants Have Identified No Compelling State Interest that Outweighs the Substantial Burden on Plaintiffs' Rights

As this Court has found, the "character and magnitude" of the state's burden

on voters' right to vote must be balanced against the state's interests. (Dkt. No. 579 at 133.) "[A]ny alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized." (*Id*. at 134 (citing *Reynolds v. Sims*, 377 U.S. 533, 562 (1964)).) "Confidence in the integrity of our electoral processes is essential to the functioning of our participatory democracy," and thus Defendants must identify the most compelling of state interests here. (*Id*. at 136 (citing *Purcell v. Gonzalez*, 549 U.S. 1, 4 (2006)).) Yet, Defendants identify no state interest whatsoever for *barcode-based* BMDs, which their own prior experts opposed. Defendants provide no reason for selecting a barcode-based BMD system when they had other options. Nor is there one. This is dispositive.

C. Defendants Fail to Show Any Burden

According to Defendants, their effort is simply too "large-scale," their voter-education efforts too "sweeping," and their expenditures too "significant" for this Court to disturb the rollout. (Opp. 49-51.) Their argument is a textbook example of the sunk-cost fallacy. And it ignores the fact that Defendants' incursion of such costs was entirely avoidable.[21] Notably, Defendants selected their barcode-based BMDs only *after* their own election security experts, Drs. Shamos and Lee, both

[21] *NEDC Opposes BMDs*, *supra* note 16 ("The initial outlay to purchase BMDs for all voters costs two or more times the cost for voting equipment used to scan hand-marked paper ballots.").

advised against those machines. They cannot now complain about timing or cost. Further, it is irrelevant how much time or money Defendants have spent *in the past* to implement the Proposed Election System. The standard for this motion asks the Court to weigh the damage *the injunction* may cause Defendants, *McDonald's Corp. v. Robertson*, 147 F.3d 1301, 1306 (11th Cir. 1998), not the damage the Defendants may have brought upon themselves by investing heavily in a system their own experts opposed. It would lead to absurd results if Defendants could avoid court-ordered relief simply by throwing good money after bad.

Defendants also ignore the actual economics. Although an injunction would trigger certain expenses unique to HMPBs, it would also yield massive savings, as Defendants would not have to roll out, maintain, house, and troubleshoot a full fleet of BMDs. Much of the $45 million Defendants spent as of November 2019 would not be wasted if Defendants are required to implement HMPBs, since the Dominion scanners can read HMPBs (*see* Dkt. No. 579 at 146), and Defendants already must prepare and print ballots for every election (Halderman Decl. ¶ 4), and Defendants must train officials to operate BMDs anyway for voters with disabilities to comply with Defendants' obligations under HAVA. In other words, the State has injected an unnecessary, very expensive, and unreliable means of voting for all but a small number of voters rather than simply using what it will be

required to have on hand in any case: paper ballots (and a small number of BMDs).

D. Curling Plaintiffs' Proposed Relief Would Best Secure the Rights of Voters with Disabilities

Defendants argue that HMPB system would trample on the rights of voters with disabilities by establishing a discriminatory voting procedure that is separate and unequal. (Opp. 30-32.) This argument is premised on a fallacy: that "Plaintiffs' legal theory is that any use of BMDs by the general public is unconstitutional and necessitates this Court's intervention." (Opp. 31.) This is not and never has been Curling Plaintiffs' legal theory, nor do Defendants cite anything indicating otherwise. Curling Plaintiffs' position is simply that Georgia's Proposed Election System, as it is being implemented by Defendants, is unconstitutional and should be enjoined. (*See*, *e.g.*, Dkt. No. 619-1 at 3 ("Curling Plaintiffs seek preliminary injunctive relief against the statewide roll-out of the ***newly chosen Dominion BMD-based system as the primary voting option*** for in-person voting for 2020 and beyond." (emphasis added)).)

Moreover, Curling Plaintiffs do not request that disabled voters be forced to use the Proposed Election System as designed. Rather, they request only that Defendants "make available at each polling place at least one electronic ***or mechanical*** BMD that is in compliance with the Americans with Disabilities Act and Help America Vote Act." (Dkt. No. 619 at 2 (emphasis added).) Curling

Plaintiffs seek additional relief intended to protect the accuracy of all votes, including those cast on proper BMDs, such as a plan for "pre-certification, post-election, manual tabulation audits of the paper ballots to verify election results, in sufficient detail for the Court to evaluate its adequacy." (*Id.*)

Defendants argue that Plaintiffs' proposed relief "can create a greater risk to election security." (Opp. 17.) This is exactly backward. Plaintiffs' proposed system would sharply reduce both the magnitude and probability of malicious interference with a small number of voters using appropriate BMDs. (Halderman Decl. ¶¶ 34-36.) That system makes it difficult or impossible for an attacker to change enough votes to swing an election result, or to do so without spurring investigation and detection. (*Cf.* Dkt. No. 554 at 87:10-13 ("if you infect a small number of machines, you have to change a lot" of votes).) In contrast, Defendants' BMDs-For-All system would massively increase the risk of outcome-changing fraud for everyone, since manipulation of only a small percentage of votes suffices to swing an election result when that manipulation is spread across a large number of voters. (Halderman Decl. ¶ 34(d).) Defendants' BMDs-For-All system will deprive all voters—including voters with disabilities—of the right to vote in a system that reliably and verifiably counts all votes.

The two premises of Defendants' security argument are also faulty.

Defendants suggest that (1) security issues would "likely be detected . . . more quickly if all voters used the BMD," and (2) limiting use of BMDs to voters with disabilities "may invite hackers . . . to target [these voters]." (Dkt. No. 658-4 ¶ 11.)[22] Defendants' first point literally is the absurd argument that the best way to detect hacking is to make *more* votes susceptible to hacking. This argument further collapses once it runs up against the reality that voters do not detect errors reliably and that there is no mechanism for individual voters to remedy systemic manipulation. (Halderman Decl. ¶¶ 22-33; Dkt. No. 640-1 at 42-43; Stark Decl. ¶¶ 11-14.) Even hyper-vigilant voters cannot detect errors on any ballots but their own, they cannot furnish evidence of vote manipulation to investigators, and *no voters* can visually confirm the accuracy of a barcode. On the second point, hackers can already target voters who use a BMD's accessible features—regardless of whether BMDs are used by all voters. (*See* Halderman Decl. ¶ 34(a); Stark Article at 6 ("the BMD 'knows' whether the voter is using the audio interface or the sip-and-puff interface").) Hackers' ability to target *any number* of voter interaction variables is exactly what makes BMDs infected with malware effectively undetectable by testing. (Stark Article at 14-15.)

Defendants and their *new* expert raise two additional arguments, neither of

[22] Mr. Riccobono rightly does not claim to be a security expert.

which withstands scrutiny. First, they assert that having only disabled voters use BMDs would threaten the secrecy of those voters' ballots because BMD-marked ballots look different than HMPBs and "[i]n many polling places, there may be a single voter with a disability using the BMD;" thus "their ballots become readily identifiable." (Dkt. Nos. 658-4 ¶ 9; 658 at 17.) But by Defendants' own admission, this scenario should rarely occur since "approximately 635,000 disabled voters cast votes in Georgia in 2016." (Dkt. No. 658-3 ¶ 40(E).) Having poll workers encourage a small number of non-disabled voters to use the BMDs would also eliminate this issue.[23] (Halderman Decl. ¶ 36.) Defendants could also implement available software-based remedies that create the appearance that BMD-produced ballots were marked by hand. (Dkt. No. 619-10 at 14.)

Defendants' remaining argument is that, if only disabled voters use BMDs, poll workers will be "less or totally unfamiliar with their set-up and operation." (Dkt. Nos. 658-4 ¶ 10; 658 at 18.) These concerns relate to the administration of voting equipment, not their technological limitations, and can be addressed through

[23] For example, an election official in Michigan, instructed her election workers to cast their own votes on accessible Dominion BMDs as part of the "inevitable learning curve" of the BMDs' roll-out. Paul Egan, *New voting machines a challenge for Michigan's blind voters*, Detroit Free Press (Aug. 6, 2018), https://www.freep.com/story/news/local/michigan/2018/08/06/voting-machines-blind-voters-michigan/887574002/.

training and testing. (Halderman Decl. ¶ 37.) Properly setting up equipment and training poll workers on accessible features are fundamental obligations that Defendants would have under any scheme of voting.

Curling Plaintiffs' proposed remedy would fully satisfy federal law, which "requires only 'reasonable modifications' that would not fundamentally alter the nature of the service provided." *Tennessee v. Lane*, 541 U.S. 509, 532 (2004). In *National Federation of the Blind v. Lamone*, 813 F.3d 494 (4th Cir. 2016), Mr. Riccobono's organization, the NFB, proposed that disabled Maryland voters be allowed to use an "online ballot marking tool" that would enable disabled voters to mark their absentee ballots electronically rather than by hand. *See id*. at 498. The Fourth Circuit affirmed this approach as a "reasonable modification" to the absentee voting system that did not "fundamentally alter" the program." *Id*. at 507-08. The relief Mr. Riccobono's organization sought in that case is completely consistent with Curling Plaintiffs' proposed relief, which calls on Defendants to supply working, accessible voting machines to certain voters as a reasonable modification, so they can participate in a secure and reliable voting system. *Id*. at 507-09. Defendants' insistence that the law requires a one-size-fits-all system contradicts recent precedent, the NFB's own prior position, and the many jurisdictions they cite that use BMDs just in the manner Curling Plaintiffs propose.

(Opp. 2; *see* Stewart Decl. Ex. 2 at 2I (63% of precincts will use BMDs primarily for voters with disabilities in November 2020).)

In *Anderson v. Franklin Institute*, 185 F. Supp. 3d 628 (E.D. Pa. 2016), the court recognized that "one of the paradoxes of the ADA" was "that the disabled must in some circumstances be treated in a way that is facially unequal in order to ensure genuine equality." *Id.* at 644. Here, "genuine equality" cannot mean that all voters must cast votes on identical machines, at the expense of the security of their votes and meaningful democracy. It must mean that all voters cast votes by methods suitable to their needs and equally benefit from a secure and accurate voting system that inspires confidence in the process and in the results. Curling Plaintiffs' proposal represents the best balance of accessibility and security that is possible with available technology. (Halderman Decl. ¶ 4.)

E. Defendants Recycle Arguments This Court Already Has Rejected or that Will Be Litigated as Part of the Motion to Dismiss

Defendants' remaining arguments are meritless. As they have before (Dkt. No. 472 at 69-70), Defendants argue that Plaintiffs seek to "upend the policy choice the State of Georgia has made," and attempt to "inappropriate[ly] use" a preliminary injunction to enact "wholesale alteration of the status quo." (Dkt. No. 658 at 36.) As discussed above, it is Defendants—not Plaintiffs—who have contravened the Georgia legislature's stated intent by choosing a voting system

that does not "produce paper ballots which are marked with the elector's choice ***in a format readable by the elector***." O.C.G.A. § 21-2-300(a)(2) (emphasis added). Moreover, a preliminary injunction is appropriate where, as here, the moving party can demonstrate the four necessary elements; maintaining the status quo is not part of the Court's calculus. (Dkt. No. 579 at 129 (citing *Robertson*, 147 F.3d at 1306).) This Court also has rejected Defendants' argument that Plaintiffs will suffer no irreparable injury absent a preliminary injunction because they are welcome to vote absentee. (*Compare* Dkt. No. 472 at 53-54, *with* Dkt. No. 658 at 47.) As this Court made clear, the injury is irreparable if the State implements or maintains a voting system that "burdens and deprives [voters] of their rights to cast secure votes that are reliably counted." (Dkt. No. 579 at 130-31.)

Defendants repeat their meritless standing arguments. (Dkt. No. 658 at 43-46.) Curling Plaintiffs maintain standing to challenge the Proposed Election System, just as with the DRE Voting System. (Dkt. No. 651 at 12-18.)

F. Fulton County Recycles Already-Rejected Arguments

Fulton County offers two primary arguments: (1) "the requested relief can only be provided by the State Defendants," and (2) Curling Plaintiff's requested relief is "essentially a second bite at the apple." (Dkt. No. 633 at 5.) These arguments are not new, and neither has merit.

i. Fulton County, as well as State Defendants, Can Provide Plaintiffs' Requested Relief

Fulton County claims Curling Plaintiffs are not entitled to injunctive relief against them because voting equipment is determined by the Secretary of State. (Dkt. No. 633 at 4.) But, as Fulton County acknowledges, "[s]tate law provides that counties . . . must conduct elections," (*id.*), and thus Curling Plaintiffs may properly seek an order directly preventing the county from conducting elections in a way that would deprive voters of their constitutional rights. *See e.g., Edge v. Sumter Cty. Sch. Dist.*, 541 F. Supp. 55, 57-58 (M.D. Ga. 1981) (enjoining county-level officials from conducting elections under at-large election system enacted by General Assembly), *aff'd,* 456 U.S. 1002 (1982).

ii. Curling Plaintiffs Do Not Seek a "Second Bite at the Apple"

Fulton County's argument that this motion is "essentially a second bite at the apple" and "tantamount to an attempt to enjoin this Court's August 15, 2019 Order" is difficult to comprehend. (Dkt. No. 633 at 5.) Fulton County evidently views the GEMS/DRE voting system as no different from the BMD-based Proposed Election System—and this of course is true with respect to fundamental vulnerabilities and unconstitutionality. But the latter has not yet been litigated. This Court's August 15, 2019 Order stated three times that it did not address the BMD system. (Dkt. No. 579 at 9 n.10, 137, 151.) The Court left open the question

of whether the Proposed Election System adequately protects voters' constitutional rights—and that is the question Curling Plaintiffs now seek to resolve. And they seek to enforce the Court's August 15, 2019 Order insofar as it established a default system for 2020 in the absence of a lawful alternative: a HMPB system.

IV. CONCLUSION

Faced with the reality that barcode-based BMDs are wholly unnecessary and thus indefensible when weighed against the substantial burdens imposed on—and potential depravation of—voters' fundamental right to vote and have their votes counted, Defendants ignore the specific election system they intend to implement statewide and instead defend BMDs generally. But this Court is not called upon to decide the constitutionality of BMDs generally. Curling Plaintiffs challenge only the specific barcode-based BMD system Defendants intend to force upon them and all other Georgia voters. For this, Defendants offer essentially no defense. This Court should enjoin Defendants from replacing one unlawful system with another and require them to implement the default system it ordered months ago: HMPBs with appropriate BMDs for those who need them or otherwise choose to use them. The Dominion scanners and election management system can readily accommodate HMPBs as proven by the Cobb County pilot. There is no reason to subject Georgia voters to a far less reliable system.

Dated: December 16, 2019

Respectfully submitted,

/s/ David D. Cross

David D. Cross (*pro hac vice*)
John P. Carlin (*pro hac vice*)
Jane P. Bentrott (*pro hac vice*)
Mary G. Kaiser (*pro hac vice*)
Robert W. Manoso (*pro hac vice*)
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue, NW
Suite 6000
Washington, DC 20006
Telephone: (202) 887-1500
DCross@mofo.com
JCarlin@mofo.com
JBentrott@mofo.com
MKaiser@mofo.com
RManoso@mofo.com

Halsey G. Knapp, Jr.
GA Bar No. 425320
Adam M. Sparks
GA Bar No. 341578
KREVOLIN & HORST, LLC
1201 West Peachtree Street, NW
Suite 3250
Atlanta, GA 30309
HKnapp@khlawfirm.com
Sparks@khlawfirm.com

Counsel for Plaintiffs Donna Curling, Donna Price & Jeffrey Schoenberg

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing document has been prepared in accordance with the font type and margin requirements of LR 5.1, using font type of Times New Roman and a point size of 14.

/s/ David D. Cross
David D. Cross

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE

I hereby certify that on December 16, 2019, a copy of the foregoing **CURLING PLAINTIFFS' REPLY IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION** was electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all attorneys of record.

/s/ David D. Cross
David D. Cross